CLAIMS

1. A home control system that uses electrical power lines for communications, comprising:

a plurality of components that are connectable for communications among themselves through the electrical power lines, said components including groups of components, wherein each group is identified collectively by a particular group identifier code;

components of any particular group being configured to compose and send messages that include the group identifier code of their particular group;

components of any particular group being further configured to receive messages from components of different groups and to disregard messages that include a group identifier code different than the group identifier code of their particular group.

2. A system as recited in claim 1, wherein the messages do not include identifiers of specific components.

3. A system as recited in claim 1, wherein:

messages composed and sent by the respective components of said particular group include first message authentication codes that are calculated using a predefined one-way function of data from the messages and of a key value that is shared between components of the particular group;

components of said particular group are configured to calculate a second message authentication code for each received message that is not disregarded, using the predefined one-way function of the data from the message and of the

shared key value, and to conclude that the received message is either not authentic or contains a data error if the first and second message authentication codes do not match.

4. A system as recited in claim 1, wherein:

the components authenticate the messages using key values that are shared between components of individual groups;

a sending one of the components is configured to change from a current to a subsequent key value in a sequence of key values without notifying a receiving component;

said receiving component automatically changing from the current to the subsequent key value if the message does not authenticate with the current key value but does authenticate with the subsequent key value;

said receiving component concluding that the received message is either not authentic or contains a data error if the message does not authenticate with the current or the subsequent key value.

5. A system as recited in claim 1, wherein:

the components authenticate the messages using key values that are shared between components of individual groups;

a sending one of the components is configured to change from a current to a subsequent key value in a sequence of key values without notifying a receiving component;

said receiving component automatically changing from the current to the subsequent key value if the message does not authenticate with the current key value but does authenticate with the subsequent key value;

said receiving component automatically changing from the current to a previous key value in the sequence of key values if the message does not authenticate with either the current key value or the subsequent key value, but does authenticate with the previous key value;

said receiving component concluding that the received message is either not authentic or contains a data error if the message does not authenticate with the previous, current, or subsequent key values.

6. A system as recited in claim 1, wherein the messages include data portions, and wherein different groups of the components use different formats for the data portions.

7. A system as recited in claim 1, wherein different groups of the components exchange data in the messages use different data exchange protocols.

8. A system as recited in claim 1, wherein:

the messages include data portions;

different groups of the components use different formats for the data portions;

different groups of the components exchange data in the messages use different data exchange protocols.

9. A system as recited in claim 1, wherein:

messages composed and sent by the respective components of said particular group include first message authentication codes that are calculated using a predefined one-way function of data from the messages and of a key value that is shared between components of the particular group;

components of said particular group are configured to calculate a second message authentication code for each received message that is not disregarded, using the predefined one-way function of the data from the message and of the shared key value, and to conclude that the received message is either not authentic or contains a data error if the first and second message authentication codes do not match;

the messages include data portions;

different groups of the components use different formats for the data portions;

different groups of the components exchange data in the messages use different data exchange protocols.

10. A electrical component that communicates with other electrical components of a particular component group using electrical power lines in a building, comprising:

a processor;

a transmitter that is responsive to the processor to send data using the electrical power lines;

the processor being programmed to compose and send messages in conjunction with the transmitter, each message including a group identifier code that is uniquely associated with the particular component group.

11. An electrical component as recited in claim 10, wherein the messages do not include identifiers of specific electrical components.

12. An electrical component as recited in claim 10, wherein messages composed and sent by the transmitter include message authentication codes that are calculated using a predefined one-way function of data from the messages and of a key value that is shared between components of the particular component group.

13. An electrical component as recited in claim 10, further comprising:

a receiver that functions in conjunction with the processor to receive messages from other electrical components using the electrical power lines;

the processor being programmed to disregard messages that include group identifier codes different than the group identifier code of said particular component group.

14. An electrical component as recited in claim 10, wherein the messages include data portions, and wherein different groups of the components use different formats for the data portions.

15. A electrical component that communicates with other electrical components of a particular component group using electrical power lines in a building, comprising:

a processor;

a receiver that functions in conjunction with the processor to receive messages from other electrical components using the electrical power lines, such messages including different group identifier codes that are associated uniquely with respective component groups;

the processor being programmed to disregard messages that include group identifier codes different than the group identifier code of said particular component group.

16. An electrical component as recited in claim 15, wherein the messages do not include identifiers of specific electrical components.

17. An electrical component as recited in claim 15, wherein:

the messages include first message authentication codes;

the processor is programmed to calculate a second message authentication code for each received message that is not disregarded, based on a predefined one-way function of the data from the message and of the shared key value, and to conclude that the received message is either not authentic or contains a data error if the first and second message authentication codes do not match.

18. An electrical component as recited in claim 15, the processor being programmed to perform steps comprising:

authenticating the messages using key values that are shared between components of respective component groups;

automatically changing from the current to the subsequent key value of a sequence of key values if a particular message does not authenticate with the current key value but does authenticate with the subsequent key value;

concluding that the received message is either not authentic or contains a data error if said particular message does not authenticate with the current or the subsequent key value.

19. An electrical component as recited in claim 15, the processor being programmed to perform steps comprising:

authenticating the messages using key values that are shared between components of respective component groups;

automatically changing from the current to the subsequent key value of a sequence of key values if a particular message does not authenticate with the current key value but does authenticate with the subsequent key value;

automatically changing from the current to a previous key value in the sequence of key values if the message does not authenticate with either the current key value or the subsequent key value, but does authenticate with the previous key value;

concluding that the received message is either not authentic or contains a data error if said particular message does not authenticate with the previous, current or subsequent key values.

20. An electrical component as recited in claim 15, wherein the messages include data portions, and wherein different groups of the electrical components use different formats for the data portions.

21. A method of communicating electronically between a plurality of electrical components using electrical power lines in a building, comprising the following steps:

designating groups of the electrical components that communicate among themselves;

assigning different group identifier codes to different groups of components;

transferring messages between components in an individual group, individual messages specifying the group identifier code of the individual group;

determining whether a particular message is intended for a particular component by checking whether the group identifier code of the particular message matches the group identifier code of the particular component's group.

22. A method as recited in claim 21, wherein the transferred messages do not include identifiers of specific electrical components.

23. A method as recited in claim 21, further comprising:

calculating first message authentication codes for the messages using a predefined one-way function of data from the messages and key values that are shared between components of individual groups;

including the first message authentication codes in the transferred messages;

calculating a second message authentication code for each message when it is received by a particular component, using the predefined one-way function of data from the message and the key value that is shared by said particular component with other components;

said particular component concluding that a received message is either not authentic or contains a data error if the calculated second message authentication code does not match the first message authentication code included in the message.

24. A method as recited in claim 21, wherein the messages include data portions, comprising a further step of using different formats for the data portions in messages transferred between components of different groups.

25. A method as recited in claim 21, comprising a further step of exchanging data in the messages using different data exchange protocols for messages transferred between components of different groups.

26. A method as recited in claim 21, further comprising:

authenticating the messages using key values that are shared between components of individual groups;

a sending one of the components of a particular group changing from a current to a subsequent key value in a sequence of key values without notifying a receiving component of the group;

said receiving component automatically changing from the current to the subsequent key value if the message does not authenticate with the current key value but does authenticate with the subsequent key value.

27. A method as recited in claim 21, further comprising:

authenticating the messages by using a message authentication code in each message, the message authentication codes being calculated using a predefined one-way function of message data and of key values that are shared between components of individual groups;

a sending one of the components of a particular group changing from a current to a subsequent key value in a sequence of key values without notifying a receiving component of the group;

said receiving component automatically changing from the current to the subsequent key value if the message does not authenticate with the current key value but does authenticate with the subsequent key value.

28. A computer-readable storage medium having instructions that are executable by an electrical component that communicates electronically using electrical power lines in a building, the instructions being executable to perform steps comprising:

composing and sending data messages over the electrical power lines;

including a group identifier code in each message, wherein the group identifier code is uniquely associated with a particular group of components that are intended to communicate with each other.

29. A computer-readable storage medium as recited in claim 28, wherein the data messages do not include identifiers of specific electrical components.

30. A computer-readable storage medium as recited in claim 28, the instructions being executable to perform further steps comprising:

calculating first message authentication codes for the data messages using a predefined one-way function of data from the messages and of a key value that is shared between components of said particular group;

including the first message authentication codes in the data messages.

31. A computer-readable storage medium as recited in claim 28, the instructions being executable to perform further steps comprising:

calculating first message authentication codes for the data messages using a predefined one-way function of data from the messages and of a key values that is shared between components of said particular group;

including the first message authentication codes in the data messages;

calculating a second message authentication code for each message when it is received by a particular component, using the predefined one-way function of data from the message and the key value that is shared by the components of said particular group;

concluding that a message is either not authentic or contains a data error if the calculated second message authentication code does not match the first message authentication code that is included in the message.

32. A computer-readable storage medium having instructions that are executable by a component that communicates electronically using electrical power lines in a building, the instructions being executable to perform steps comprising:

receiving messages from other electrical components using the electrical power lines, such messages including different group identifier codes;

disregarding messages that include a group identifier code different than a group identifier code is uniquely associated with a particular group of components that are intended to communicate with each other.

33. A computer-readable storage medium as recited in claim 32, wherein the messages do not include identifiers of specific electrical components.

34. A computer-readable storage medium as recited in claim 32, wherein messages composed and sent by the transmitter include first message authentication codes, the instructions being executable to perform further steps comprising:

calculating a second message authentication code for each received message based on a predefined one-way function of the data from the message and of a key value that is shared between components of said particular component group;

concluding that the message is either not authentic or contains a data error if the first and second message authentication codes do not match.

35. A home control system that uses electrical power lines for communications, comprising:

a plurality of components that are connected for communications among themselves through the electrical power lines;

a sending one of the components being configured to send messages over the electrical power lines in accordance with steps comprising:

calculating a first message authentication code based on a predefined one-way function of data from a message and of a key value that is shared between sending and receiving components;

including the message authentication code in the message;

sending the message over the electrical power lines;

a receiving one of the components being configured to receive messages in accordance with steps comprising:

receiving a message over the electrical power lines;

calculating a second message authentication code based on the predefined one-way function of the data from the message and of the a current shared key value;

concluding that the message is either not authentic or contains a data error if the first and second message authentication codes do not match.

36. A home control system as recited in claim 35, wherein the shared key value is from a sequence of key values;

the sending component being further configured to change from a current to a subsequent key value in the sequence without notifying the receiving component;

the receiving component being further configured to calculate a third message authentication code based on the predefined one-way function of the data from the message and of the subsequent key value;

the receiving being further configured to change from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

37. A home control system as recited in claim 35, wherein the shared key value is from a sequence of key values;

the sending component being further configured to change from a current to a subsequent key value in the sequence without notifying the receiving component;

the receiving component being further configured to calculate a third message authentication code based on the predefined one-way function of the data from the message and of the subsequent key value;

the receiving being further configured to change from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match;

wherein the sending and receiving components calculate the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

38. A home control system as recited in claim 35, wherein the shared key value is from a sequence of key values, and wherein the sending and receiving components calculate the sequence of key values using a one-way function of counter values that advance to generate each sequential key value.

39. A electrical component that is connected for communications with other electrical components of a particular group using electrical power lines in a building, comprising:

a processor;

a transmitter that is responsive to the processor to send data using the electrical power lines;

the processor being programmed to compose and send messages in conjunction with the transmitter, each message including a message authentication code based on a predefined one-way function of data from the message and of a key value that is shared between a plurality of components.

40. An electrical component as recited in claim 39, wherein the shared key value is from a sequence of key values, the processor being further programmed to change from a current to a subsequent key value in the sequence without notifying a receiving component.

41. An electrical component as recited in claim 39, wherein the shared key value is from a sequence of key values, wherein the processor calculates the sequence of key values using a one-way function of a counter values that advance to generate each sequential key value.

42. A electrical component that is connected for communications with other electrical components of a particular group using electrical power lines in a building, comprising:

a processor;

a receiver that functions in conjunction with the processor to receive messages from other electrical components using the electrical power lines, such messages including first message authentication codes;

the processor being programmed to calculate a second message authentication code for each message based on a predefined one-way function of the data from the message and of a key value that is shared between a plurality of components;

the processor being further programmed to compare the first and second message authentication codes to authenticate each message.

43. An electrical component as recited in claim 42, wherein the shared key value is from a sequence of key values, the processor programmed to perform the following steps:

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a subsequent key value in the sequence of key values;

further comparing the first and third message authentication codes to authenticate each message.

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

44. An electrical component as recited in claim 42, wherein the shared key value is from a sequence of key values, the processor programmed to perform the following steps:

calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value;

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a subsequent key value in the sequence of key values;

further comparing the first and third message authentication codes to authenticate each message.

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

45. An electrical component as recited in claim 42, wherein the shared key value is from a sequence of key values, wherein the processor calculates the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

46. A method of communicating electronically between a plurality of electrical components using electrical power lines in a building, comprising the following steps:

designating groups of the electrical components that communicate among themselves;

sharing a key value between components of a particular group;

calculating a first message authentication code based on a predefined one-way function of data from a message and of the key value that is shared by components of the particular group;

including the message authentication code in the message;

sending the message over the electrical power lines;

receiving the message;

calculating a second message authentication code based on the predefined one-way function of the data from the message and of the shared key value;

comparing the first and second message authentication codes to authenticate each message.

47. A method as recited in claim 46, wherein the shared key value is from a sequence of key values, the method further comprising an additional step of changing from a current to a subsequent key value in the sequence without notifying receiving components.

48. A method as recited in claim 46, wherein the shared key value is from a sequence of key values, the method further comprising:

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a subsequent key value in the sequence of key values;

further comparing the first and third message authentication codes to authenticate each message.

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

49. A method as recited in claim 46, wherein the shared key value is from a sequence of key values, the method further comprising:

calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value;

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a subsequent key value in the sequence of key values;

further comparing the first and third message authentication codes to authenticate each message;

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

50. A method component as recited in claim 46, wherein the shared key value is from a sequence of key values, further comprising a step of calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

51. A method as recited in claim 46, further comprising:

assigning different group identifier codes to different groups of components;

specifying the group identifier code of an individual group in messages sent to components of said individual group;

determining whether a particular message is intended for a particular component by checking whether the group identifier code of the particular message matches the group identifier code of the particular component's group.

52. A computer-readable storage medium having instructions that are executable by an electrical component that communicates electronically using electrical power lines in a building, the instructions being executable to perform steps comprising:

calculating a message authentication code based on a predefined one-way function of data from a message and of a key value that is shared by components of a particular group of electrical components;

including the message authentication code in the message;

sending the message over the electrical power lines.

53. A computer-readable storage medium as recited in claim 52, wherein the shared key value is from a sequence of key values, the instructions being executable to perform further steps comprising a step of changing from a current to a subsequent key value in the sequence without notifying other components.

54. A computer-readable storage medium as recited in claim 52, wherein the shared key value is from a sequence of key values, the instructions being executable to perform a further step of calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

55. A computer-readable storage medium having instructions that are executable by an electrical component that communicates electronically using electrical power lines in a building, the instructions being executable to perform steps comprising:

receiving a message that contains a first message authentication code;

calculating a second message authentication code based on a predefined one-way function of data from the message and of a key value that is shared by a plurality of electrical components;

concluding that the message is either not authentic or contains a data error if the first and second message authentication codes do not match.

56. A computer-readable storage medium as recited in claim 55, wherein the shared key value is from a sequence of key values, the instructions being executable to perform a further steps comprising:

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a key value in the sequence of key values that is subsequent to a current key value;

further comparing the first and third message authentication codes to authenticate each message;

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match;

57. A computer-readable storage medium as recited in claim 55, the instructions being executable to perform a further step of calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.